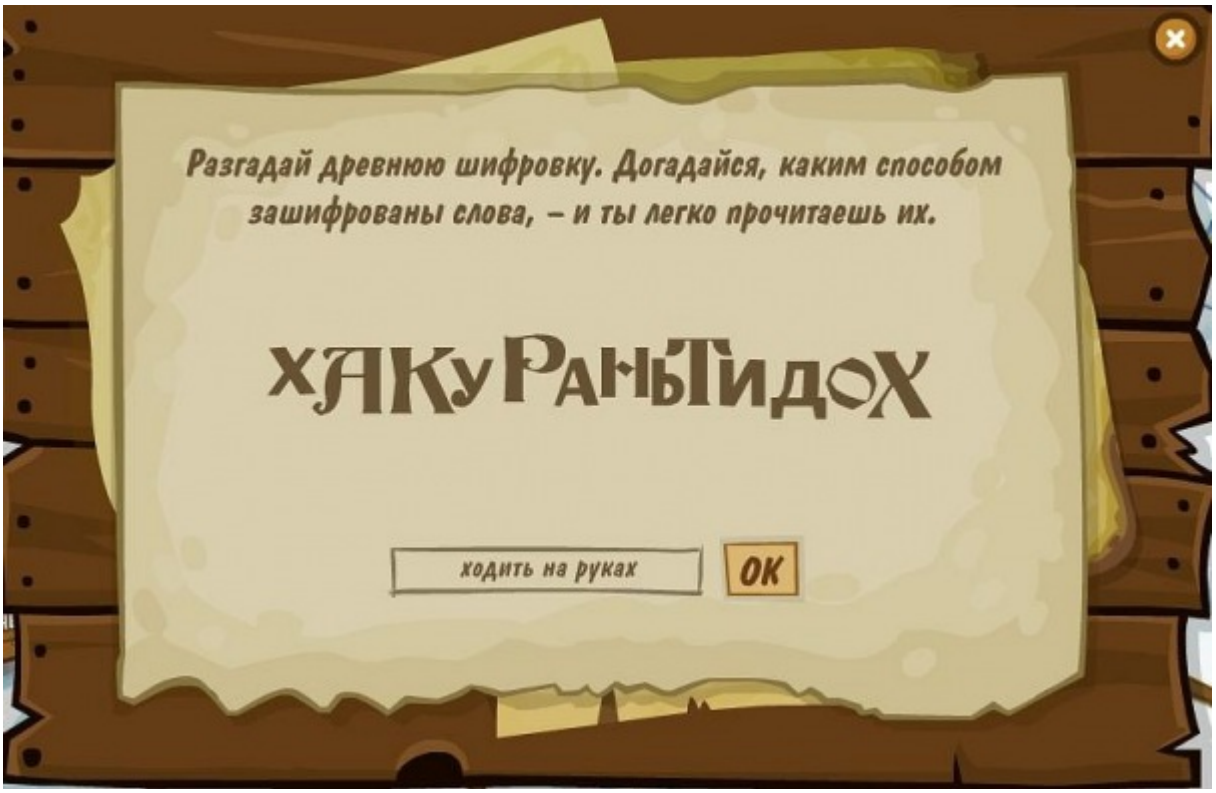
Перестановочные шифры

Простая перестановка

Простая перестановка без ключа — один из самых простых методов шифрования. Буквы перемешиваются по каким-либо правилам, но эти правила могут быть разными — и простыми и сложными.

Транспозиция

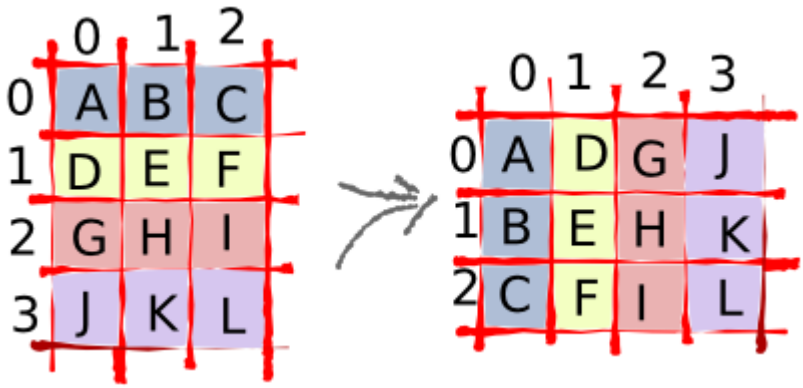
Допустим, у нас есть фраза: **«МОЖНО, НО НЕЛЬЗЯ»**. И мы хотим её зашифровать. Самый простой способ - это записать всю фразу задом наперёд: **«ЯЗЬЛЕН ОН, ОНЖОМ»**. Можно порядок слов в предложении оставить исходным, но каждое слово записать задом наперёд: **«ОНЖОМ, ОН ЯЗЬЛЕН»**. А можно менять местами каждые две буквы: **«ОМНЖ,ООНЕНЬЛЯЗ»**. Это называется «транспозиция» или простая перестановка в чистом виде.



Транспонирование

В этом шифре используется таблица. Сообщение записывается в таблицу по строкам, а для образования шифрованного текста считывается по столбцам. Ну или наоборот - записывается на столбцам, а считывается по строкам. Мы как бы переворачиваем таблицу относительно её диагонали, проходящей через верхний левый и нижний правый углы. Математики называют такой способ переворота таблицы транспонированием.

Для шифрования нужно нарисовать подходящего размера таблицу, вписать туда построчно шифруемый текст, а затем выписать его по столбцам в одну строку. Для расшифровки нужно лишь будет сообщить ключ шифра в виде размера таблицы. На рисунке ниже из **ABCDEFGHIJKL** получается **ADGJBEHKCFIL**. Согласитесь, понять без картинки, что это был алфавит, уже практически невозможно.



Итак, например, нам нужно зашифровать текст ***«Я памятник себе воздвиг нерукотворный, к нему не зарастёт народная тропа»***. В нём 72 символа. 72 - удобное число, оно делится без остатка на 2,4,6,8,12,18,24,36, поэтому можно использовать таблицы 2x36, 3x24, 4x18, 6x12, 8x9, 9x8, 12x6, 18x4, 24x3, 36x2 :). Определяемся с ключом (размером таблицы), вписываем текст по строкам, а затем переписываем его по столбцам.

1)

	1	2	3	4	5	6	7	8	9
1	Я	.	п	а	м	я	т	н	и
2	к	.	с	е	б	е	.	в	о
3	з	д	в	и	г	.	н	е	р
4	у	к	о	т	в	о	р	н	ы
5	й	,	.	к	.	н	е	м	у
6	.	н	е	.	з	а	р	а	с
7	т	ё	т	.	н	а	р	о	д
8	н	а	я	.	т	р	о	п	а

2)

	1	2	3	4	5	6	7	8
1	Я	.	п	а	м	я	т	н
2	и	к	.	с	е	б	е	.
3	в	о	з	д	в	и	г	.
4	н	е	р	у	к	о	т	в
5	о	р	н	ы	й	,	.	к
6	.	н	е	м	у	.	н	е
7	.	з	а	р	а	с	т	ё
8	т	.	н	а	р	о	д	н
9	а	я	.	т	р	о	п	а

3)

	1	2	3	4
1	Я	.	п	а
2	м	я	т	н
3	и	к	.	с
4	е	б	е	.
5	в	о	з	д
6	в	и	г	.
7	н	е	р	у
8	к	о	т	в
9	о	р	н	ы
10	й	,	.	к
11	.	н	е	м
12	у	.	н	е
13	.	з	а	р
14	а	с	т	ё
15	т	.	н	а
16	р	о	д	н
17	а	я	.	т
18	р	о	п	а

4)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	Я	.	п	а	м	я	т	н	и	к	.	с	е	б	е	.	в	о
2	з	д	в	и	г	.	н	е	р	у	к	о	т	в	о	р	н	ы
3	й	,	.	к	.	н	е	м	у	.	н	е	.	з	а	р	а	с
4	т	ё	т	.	н	а	р	о	д	н	а	я	.	т	р	о	п	а

На рисунке выше показаны варианты с таблицами 9×8, 8×9, 4×18 и 18×4. Для третьего варианта (таблица 4×18) получится вот такой текст:

«Ямиеввнкой у атрар якбоиеор,н зс ояопт езгртн енатнд панс д увыкмерёанта (4:18)»

В данном случае я взял текст «как есть», то есть с пропусками между словами и со знаками препинания. Но если текст осмысленный, то знаки препинания и пропуски между словами можно и не использовать.

Штакетник

Упрощённый вариант транспонирования (с двухстрочной таблицей) - «штакетник». Напоминает «по конструкции» забор-шахматку.

Это очень простой способ шифровки, часто применяемый школьниками. Фраза записывается в две строки: в верхней пишутся нечётные буквы, в нижней - чётные. Затем нужно выписать подряд сначала верхнюю строку, затем нижнюю. Такое шифрование легко проделать и в уме, не выписывая сначала две строки.

«Я памятник себе воздвиг нерукотворный» превращается в «ЯАЯНКЕЕОДИНРКТОНЙ ПМТИСБВЗВГЕУОВРЫ».

Я		А		Я		Н		К		Е		Е		О		Д		И		Н		Р		К		Т		О		Н		Й
	П		М		Т		И		С		Б		В		З		В		Г		Е		У		О		В		Р		Ы		

Скитала

Известно, что в V веке до нашей эры правители Спарты, наиболее воинственного из греческих государств, имели хорошо отработанную систему секретной военной связи и шифровали свои послания с помощью «скиталы», первого простейшего криптографического устройства, реализующего метод простой перестановки.

Шифрование выполнялось следующим образом. На стержень цилиндрической формы, который и назывался «скитала», наматывали спиралью (виток к витку) полоску пергамента и писали на ней вдоль стержня несколько строк текста сообщения. Затем снимали со стержня полоску пергамента с написанным текстом. Буквы на этой полоске оказывались расположенными хаотично. Для восстановления текста требовалась скитала такого же диаметра.

По сути скитала - это наша обычная плоская таблица, обёрнутая вокруг цилиндра.

Считается, что автором способа взлома шифра скиталы является Аристотель, который наматывал ленту на конусообразную палку до тех пор, пока не появлялись читаемые куски текста. Изначально древний аппарат использовался в качестве сохранения секретных рецептов. Сейчас вместо узкой полоски пергамента можно использовать серпантин, а роль скиталы выполнит карандаш.

Сдвиг

Похожий результат можно получить, если буквы сообщения писать через определенное число позиций до тех пор, пока не будет исчерпан весь текст. Ниже пример готовой головоломки, составленной по таким правилам.

«Три дробь четыре» - это подсказка, что зашифровано три слова, читать надо каждую четвёртую букву (4-8-12-16-..), по достижению конца переходить снова к началу со сдвигом на 1 букву влево (3-7-11-15-..) и т.д. На рисунке ниже зашифровано «Идите назначенным маршрутом».

Одиночная перестановка по ключу

Более практический метод шифрования, называемый одиночной перестановкой по ключу, очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы не сдвигаются, а переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Кодируемая фраза записывается в подходящую таблицу построчно. Затем над таблицей вставляется пустая строка и в неё вписывается ключевое слово/фраза/последовательность чисел. Затем это ключевое слово/фраза/последовательность сортируется по алфавиту/значению, вместе с ней сортируются столбцы, тем самым перемешивая всю таблицу. Затем зашифрованная фраза выписывается построчно из этой перемешанной таблицы.

1	2	3	4	5	6	7	8	9
	У	Р	О	М	К	У	Л	О
Ь	У	Ё	З	Е	Б	Я	Д	Л
Н	З	Я	А	Т	Л	Ы	Й	А
Ц	Ь	Б	А	Д	Н	Е	П	У
Е	М	М	Д	Н	И	Т	О	Ё
И	Ч	Т	Ю	К	Ь	Н	О	О
У	Н	Ё	Й	В	Ы	Ч	Ё	С
Х	И	Е	П	О	Т	О	Д	Ц
П	Р	М	Г	О	У	И	К	

8	9		4			2	5	
		2		5	6			7
		4			1	3		
	4	5	3		9		8	
	7			6			9	
	2			8		4	1	
		9	6			1		
4			1	3		8		
	8	1			2		3	4

8	9	6	4	7	3	2	5	1
3	1	2	8	5	6	9	4	7
7	5	4	9	2	1	3	6	8
6	4	5	3	1	9	7	8	2
1	7	8	2	6	4	5	9	3
9	2	3	5	8	7	4	1	6
2	3	9	6	4	8	1	7	5
4	6	7	1	3	5	8	2	9
5	8	1	7	9	2	6	3	4

1	7	8	2	6	4	5	9	3
	У	Л	У	К	О	М	О	Р
Ь	Я	Д	У	Б	З	Е	Л	Ё
Н	Ы	Й	З	Л	А	Т	А	Я
Ц	Е	П	Ь	Н	А	Д	У	Б
Е	Т	О	М	И	Д	Н	Ё	М
И	Н	О	Ч	Ь	Ю	К	О	Т
У	Ч	Ё	Н	Ы	Й	В	С	Ё
Х	О	Д	И	Т	П	О	Ц	Е
П	И	К	Р	У	Г	О		М

Например, можно сделать головоломку на основе судоку. Разгадывающему даётся текст «-УРОМКУЛО ЬУЁЗЕБЯДЛ НЗЯАТЛЫЙА ЦЬБАДНЕПУ ЕММДНИТОЁ ИЧТЮКЬНОО УНЁЙВЫЧЁС ХИЕПОТОДЦ ПРМГОУИК-» и предлагается решить судоку, в которой одна из строк помечена.

Решать эту головоломку придётся так: сначала нужно записать текст в таблицу 9×9, затем разгадать судоку, нарисовать пустую таблицу 9×9, надписать над ней ключевую строку из помеченной строки, и затем в таблицу под номерами вписать столбцы согласно их порядковым номерам в исходной таблице.

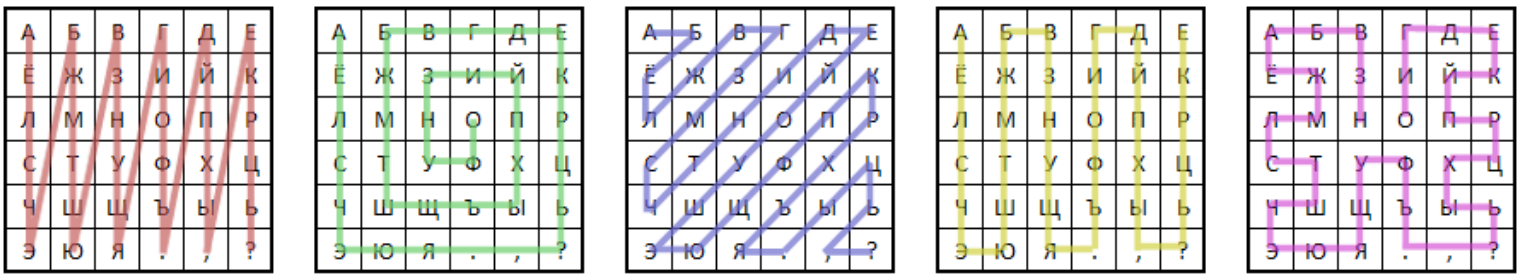
Для детей можно использовать этот же метод, но попроще, даже без цифр, а сразу нарисовав порядок перестановки в виде путей.

Двойная перестановка

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием «двойная перестановка». Для этого размер второй таблицы подбирают так, чтобы длины её строк и столбцов были не такие, как в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки.

Маршрутная перестановка

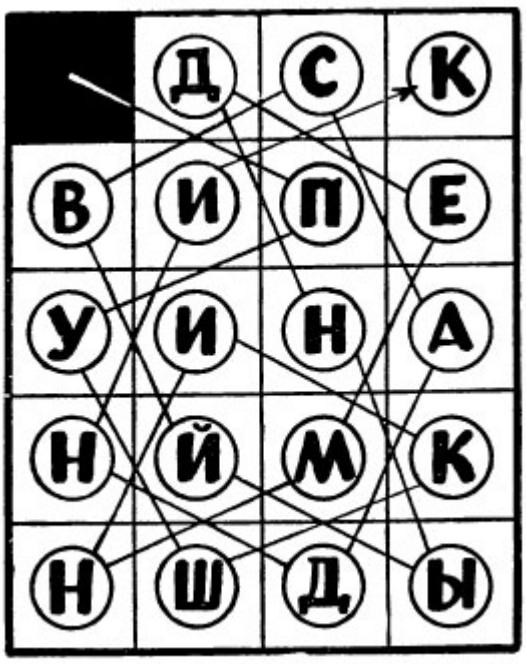
Обычное транспонирование таблицы (заполняем по строкам, читаем по столбцам) можно усложнить и считывать не по столбцам, а змейкой, зигзагом, по спирали или каким-то другим способом, т.е. задавать маршрут обхода таблицы. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным. Правда, процесс расшифровки при этом усложняется, особенно, если маршрут неизвестен, и его ещё надо узнать.



На рисунке сверху последовательность символов «АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.,?» вписана построчно в таблицу 6×6, а затем считана по маршруту, указанному линиями. Получаются следующие шифровки:

АЁЛСЧЭБЖМТШЮВЗНУЩЯГИОФЪ.ДЙПХЫ,ЕКРЦЬ?
АЁЛСЧЭЮЯ.,?ЬЦРКЕДГВБЖМТШЩЪЫХПЙИЗНУФО
АБЁЛЖВГЗМСЧТНИДЕЙОУШЭЮЩФПКРХЪЯ.ЫЦЬ,?
АЁЛСЧЭЮШТМЖБВЗНУЩЯ.ЪФОИГДЙПХЫ,?ЬЦРКЕ
НЗВБАЁЖМЛСТШЧЭЮЯЩУФЪ.,?ЬЫХЦРПЙКЕДГИО

А здесь нужно обходить таблицу «ходом коня», причём маршрут уже нарисован, так что это совсем для маленьких :)

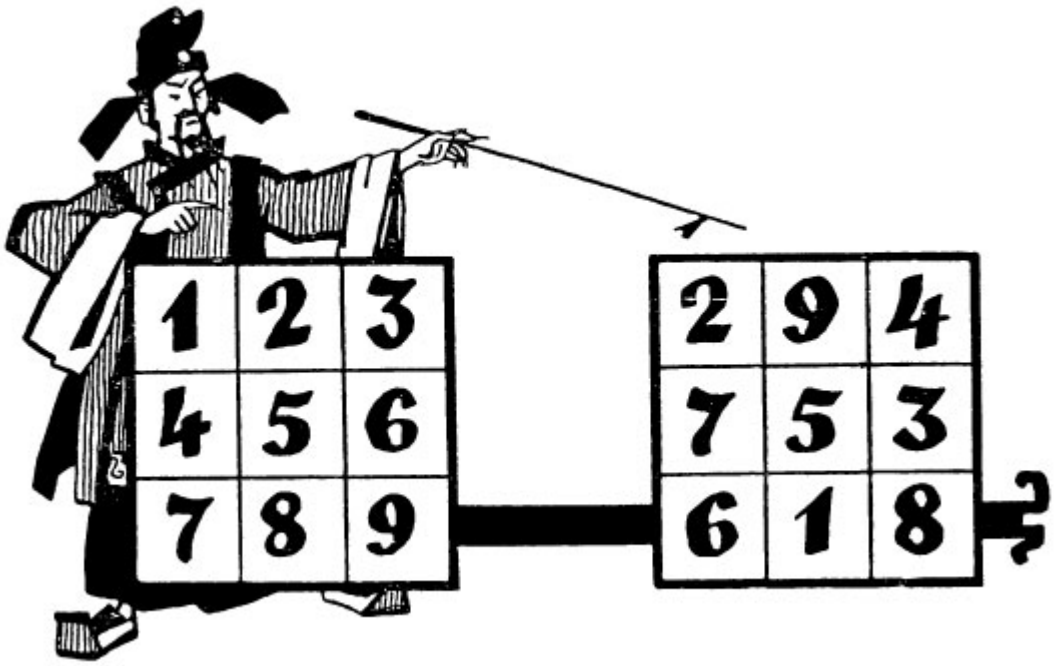


Но если подать эту головоломку так, как показано ниже, то будет уже совсем не просто, так как вариантов обхода ходом коня может быть много, и нужно будет найти из всех этих вариантов единственный правильный.

Зашифровано «Пушкин. Медный всадник».

Перестановка "Волшебный квадрат"

Волшебными (или магическими) квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1 до n^2 (где n - размерность квадрата), которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.



В известном ещё в Древнем Китае квадрате Ло-Шу третьего порядка (3×3) константа квадрата 15 повторяется 8 раз:

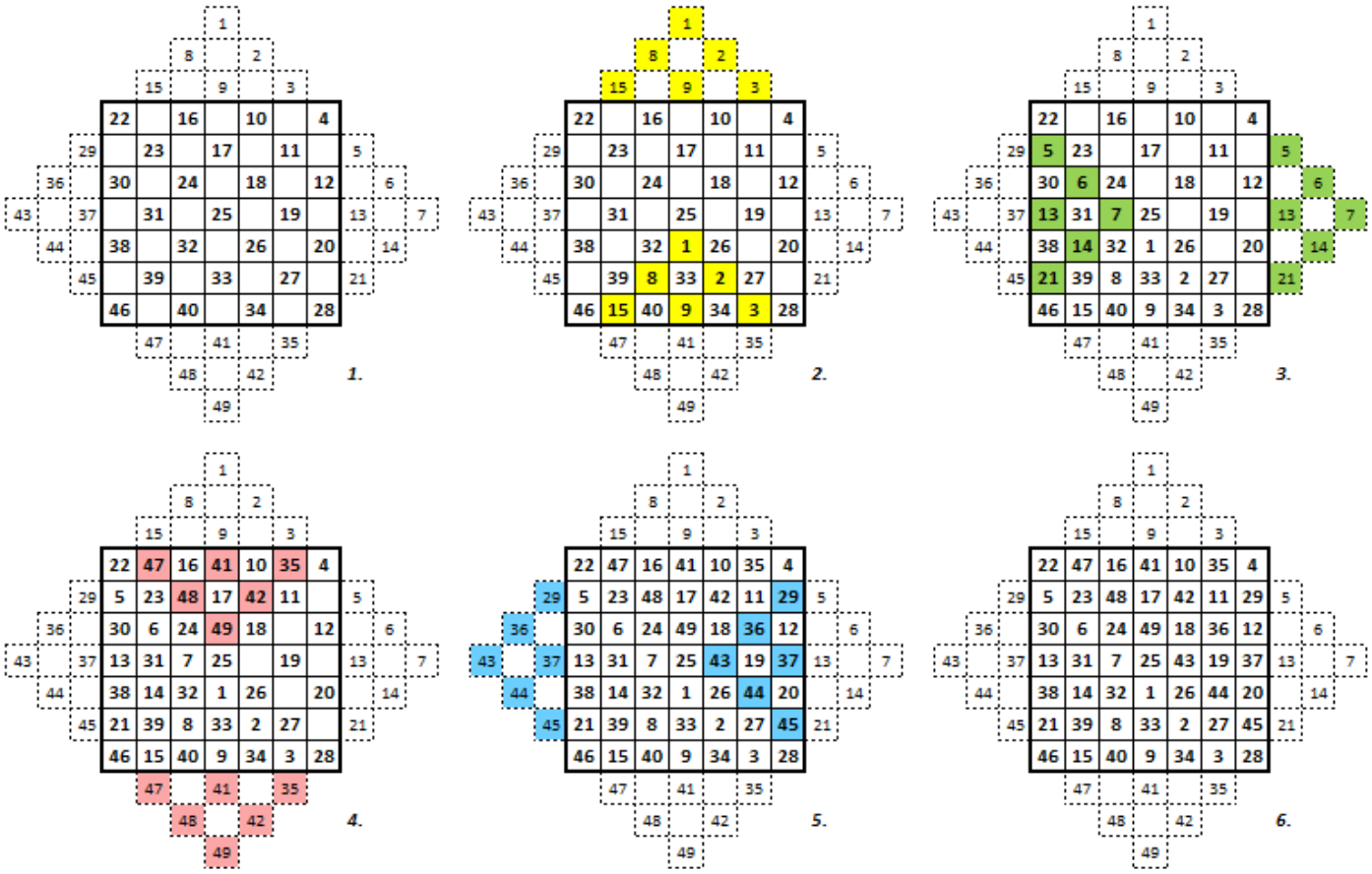
1. по трём горизонталям: 2+9+4 = 7+5+3 = 6+1+8 = 15
2. по трём вертикалям: 2+7+6 = 9+5+1 = 4+3+8 = 15
3. по двум диагоналям: 2+5+8 = 4+5+6 = 15

Кстати, константу нечетного квадрата легко посчитать, умножив среднее число ряда, из которого составлен квадрат, на порядок квадрата. Для квадрата 3-го порядка (3×3) константа равна $_{1234}\mathbf{5}_{6789}$*3=15.

Далее, чтобы зашифровать какое-то послание, нужно сначала подобрать или составить подходящий по размеру волшебный квадрат, затем нарисовать пустую таблицу такого же размера, и вписать буквы текста по очереди в таблицу в соответствии с номерами в волшебном квадрате. Затем просто выписываем построчно буквы из таблицы в одну длинную строку. Порядок квадрата должен быть равен округлённому в большую сторону корню из длины шифруемой строки, чтобы строка полностью вошла в квадрат. Если строка короче, то остаток можно заполнить произвольными буквами или цифрами.

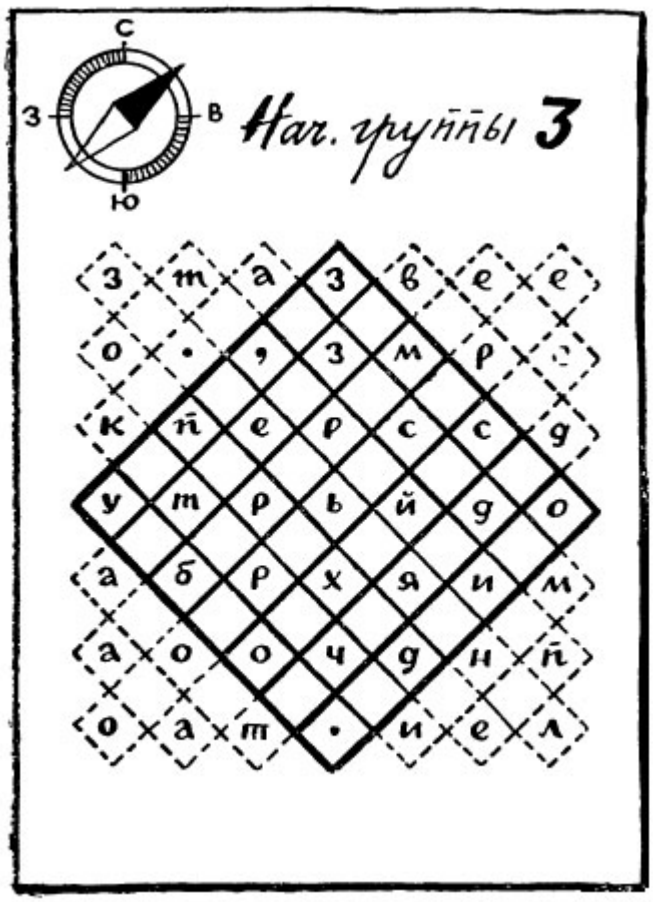
На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3x3, если не принимать во внимание его повороты и отражения. Счёт волшебным квадратам 4-го порядка уже идёт на сотни, 5-го - на сотни тысяч. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, так как ручной перебор всех вариантов ключа для этого шифра был немыслим.

Есть очень простой метод составления нечётных волшебных квадратов, т.е. размером 3×3, 5×5, 7×7 и т.д. Это метод «террас» или «пирамидок».



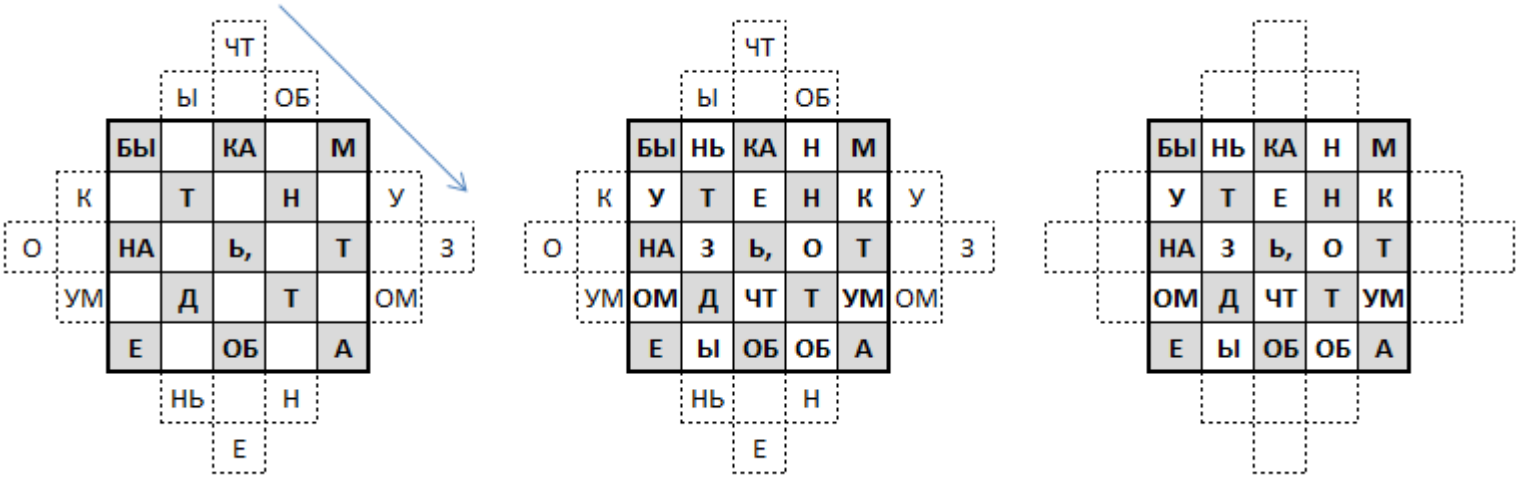
Рисуется квадрат нужного размера и к нему пририсовываются ступенчатые «террасы» (обозначены пунктиром). Далее по диагоналям сверху вниз направо квадрат заполняется последовательными числами. После этого «террасы» переносятся внутрь квадрата: правые - налево, левые - направо, верхние - вниз, а нижние - наверх. Получается волшебный квадрат!

На базе этого метода можно составлять разные головоломки. Если использовать метод напрямую, то получится вот такая головоломка:



Чтобы решить эту головоломку, нужно буквы из «террас» перенести в квадрат, тогда в квадрате прочитается полное сообщение. Здесь зашифрована фраза «За мостом засада, пройти нельзя, переходите речку в брод.»

А если использовать метод наоборот, то получится головоломка типа такой.



Чтобы её решить, надо вытащить соответствующие буквы из квадрата в «террасы».

Для квадратов 4×4, 6×6 и т.д. таких простых способов их составления не существует, поэтому проще использовать готовые. Например, квадрат Дюрера.

Вращающаяся решётка

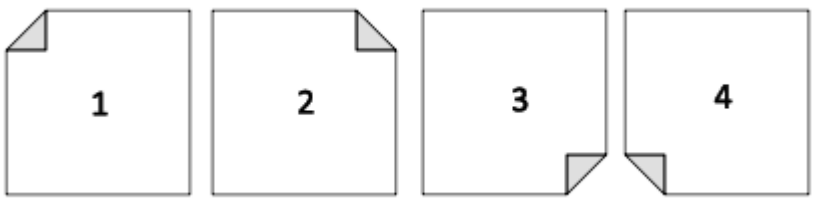
Классическая **решётка Кардано** позволяет скрыть шифровку внутри мусорного текста и является хорошим примером **стеганографии**. Но если решётку Кардано использовать в качестве ключа для перестановочного шифра, то получим новый метод шифрования — вращающуюся решётку или сетку.

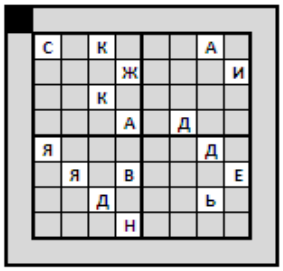
Решётка — это квадрат размером NxN клеток, некоторые из которых вырезаны. Вырезанные клетки могут касаться друг друга, в том числе вершинами, и даже сторонами. В одной клетке — одна буква. Вырезанные клетки должны располагаться таким образом, чтобы никакие две из них не оказывались в одном и том же месте при поворотах решётки.

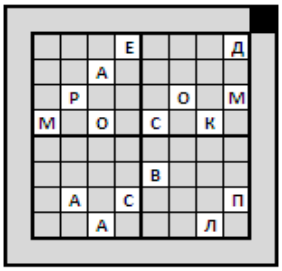
При помощи конструктора, изображённого ниже, можно изготовить 4^{16} (4 294 967 296) таких решёток. Для этого нужно вырезать строго одно из четырёх повторяющихся чисел. Для шифрования без мусора нужно вырезать все номера от 1 до 16, всего 16 клеток. Для шифрования с мусором некоторые числа можно не вырезать, оставшиеся места после шифрования заполнить любыми произвольными буквами, это и будет мусор.

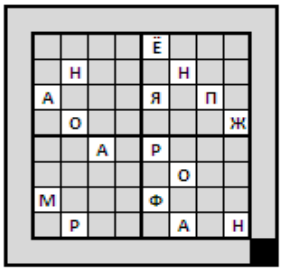
1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

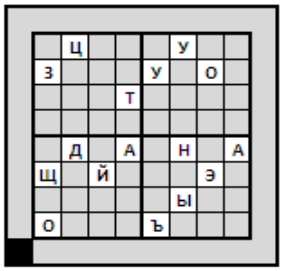
Использовать полученную решётку надо следующим образом. Положить решётку на бумагу и в вырезанные клетки по одной букве начать вписывать шифруемый текст. Как только 16 букв будет вписано, решётка поворачивается на 90°, и вписываются следующие 16 букв, и так ещё два раза. В результате будет вписано 64 буквы. Если текст был короче, то в оставшиеся на бумаге пустые места нужно вписать произвольные буквы. Более длинный текст можно разбить на части по 64, и шифровать каждую отдельно. А можно вписывать в окошки и по две буквы.











Есть второй способ перекладывания решётки во время шифрования — не поворачивать решётку на 90° три раза, а в первый раз повернуть её на 180°, второй раз перевернуть обратной стороной относительно горизонтальной оси, в третий раз - снова повернуть на 180°.